UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

ROBIN GUERTIN, on behalf of herself and all others similarly situated, Plaintiff, v. ONETOUCHPOINT MIDWEST CORP., Defendant.	Case No. 2:22-cv-899 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Complaint against the Defendant, OneTouchPoint Midwest Corp. ("OTP" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, alleging as follows:

INTRODUCTION

1. OTP, a Wisconsin-based marketing and managed services provider, lost control over consumers' highly sensitive personal information in a data breach by cybercriminals ("Data Breach").

2. On April 28, 2022, OTP discovered encrypted files on certain of its computer systems. An investigation determined that an unauthorized third party obtained access to OTP's servers beginning as of April 27, 2022 (the "Data Breach"). Starting on June 3, 2022, OTP began notifying its business customers of the Data Breach. OTP waited another two months to start notifying persons whose personal and confidential information had been compromised of the Data Breach.

3. The compromised information includes "protected health information" ("PHI"), including consumers' health records and assessments.

4. OTP's misconduct violates state and federal and industry standard data security policies. Indeed, the Data Breach shows that OTP's data security could not prevent, detect, or stop the Data Breach before cybercriminals could bypass OTP's and access consumers' PHI.

5. Plaintiff is a Data Breach victim who, prior to receiving notice that she is a data breach victim, had never heard of OTP. It appears OTP obtained her PHI in performing marketing services for Plaintiff's healthcare insurer or provider. Plaintiff brings this Class Action on behalf of herself, and all others harmed by OTP's misconduct.

PARTIES

6. Plaintiff, Robin Guertin, is a natural person and citizen of South Carolina, residing in Manning, South Carolina, where she intends to remain. Guertin has used Humana for healthcare services and upon information and belief, OTP collects Humana's data to perform its marketing services. Guertin is a Data Breach victim, having received OTP's breach notice letter on August 4, 2022.

7. Defendant, OTP, is a Wisconsin corporation with its principal place of business at 125 Walnut Ridge Drive, Hartland, WI 53029.

JURISDICTION & VENUE

8. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

9. This Court has personal jurisdiction over Defendant because it is incorporated in Wisconsin and its principal place of business is located in Wisconsin.

10. Venue is proper because Defendant's headquarters are located in this District.

BACKGROUND FACTS

a. OTP

11. OTP is a marketing and brand management company whose customers include Fortune 500 companies in the manufacturing, franchise, retail, healthcare and financial services industries.

12. In providing marketing services to healthcare providers, those providers entrust OTP with confidential patient information.

13. OTP promises that it "adhere[s] to the strictest HIPAA standards and ensure[s] that the handling of protected health information (PHI) is secure."[1]

b. OTP Fails to Safeguard PHI and PII

14. Plaintiff is a consumer who uses Humana for healthcare related services. Upon information and belief Humana is one of OTP's customers.

15. As a condition to receiving services, OTP requires its customers to disclose PHI and PII in the customers' systems, including consumers' names, dates of birth, health assessment records and related information.

16. OTP collects and maintains PHI and PII in its computer systems.

17. In collecting and maintaining the PHI and PII, OTP is obligated by law and its own internal policies to safeguard the data.

18. On April 28, 2022, OTP discovered encrypted files on certain of its computer systems. An investigation determined that an unauthorized third party obtained access to OTP's servers beginning as of April 27, 2022. On June 1, 2022, OTP learned that it would be unable to determine which files the third party illegally accessed in its system. Starting on June 3, 2022, OTP

[1] https://1touchpoint.com/solutions/healthcare (last accessed Aug. 7, 2022).

began notifying its business customers of the Data Breach.

19. OTP's website lists 34 healthcare customers whose patients' PII and PHI may have been compromised.[2]

20. In early August 2022, OTP finally started notifying persons whose PII and PHI had been compromised of the Data Breach. A true and correct copy of the notice letter Plaintiff received is attached hereto as **Exhibit A** (the "Breach Notice").

21. On information and belief, OTP failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PHI and PII. OTP's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PHI and PII. Further, the Breach Notice makes clear that OTP has not determined the full scope of the Data Breach, as it has disclosed scant detail regarding the Data Breach.

c. Plaintiff's Experience

22. Plaintiff's PHI and PII was disclosed to Humana and, upon information and belief, Humana shared this PHI and PII with OTP.

23. Plaintiff provided her PHI and PII trusting that it would be protected.

24. Plaintiff learned that her PHI had been compromised in the Data Breach only when she received the Breach Notice on August 4, 2022.

25. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

[2] https://1touchpoint.com/notice-of-data-event (last accessed Aug. 6, 2022).

26. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect himself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

27. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

28. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

29. Plaintiff has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

30. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

31. Plaintiff and members of the proposed Class have suffered injury from the misuse

of their PHI and PII that can be directly traced to Defendant.

32. As a result of OTP's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PHI and PII is used;

b. The diminution in value of their PHI and PII;

c. The compromise and continuing publication of their PHI and PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PHI and PII; and

h. The continued risk to their PHI and PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PHI and PII in their possession.

33. Stolen PHI and PII are one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI and PII can be worth up to $1,000.00 depending on the type of information obtained.

34. The value of Plaintiff's and the proposed Class's PHI and PII on the black market is considerable. Stolen PHI and PII trades on the black market for years, and criminals frequently

post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

35. It can take victims years to spot identity or PHI and PII theft, giving criminals plenty of time to use that information for cash.

36. One such example of criminals using PHI and PII for profit is the development of "Fullz" packages.

37. Cyber-criminals can cross-reference two sources of PHI and PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

38. The development of "Fullz" packages means that stolen PHI and PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI and PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PHI and PII is being misused, and that such misuse is fairly traceable to the Data Breach.

39. Defendant disclosed the PHI and PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PHI and PII of Plaintiff and members of the proposed Class to people

engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PHI and PII.

40. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and proposed Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendant failed to adhere to FTC guidelines.

41. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PHI and PII.

42. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

43. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

44. The FTC recommends that companies not maintain information longer than is

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

f. Defendant Failed to Comply with HIPAA.

47. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

48. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

49. The Data Breach itself resulted from a combination of inadequacies showing OTP failed to comply with safeguards mandated by HIPAA. OTP's security failures include, but are

not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by OTP's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3) on behalf of herself and all members of the proposed class ("Class"), defined as follows:

All individuals residing in the United States whose PHI or PII was compromised in the Data Breach disclosed by OTP in the Breach Notice.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

51. Plaintiff reserves the right to amend the class definition.

52. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The exact number of the members of the Class is unknown but, upon information and belief, the number is likely in the thousands and individual joinder in this case is impracticable.;

b. **Ascertainability**. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PHI and PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PHI and PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's PHI and PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

53. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

54. Plaintiff reallege all previous paragraphs as if fully set forth below.

55. Plaintiff and members of the Class entrusted their PHI and PII to Defendant, as a third party working with their health care or health insurance providers. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PHI and PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

56. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PHI and PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI and PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's PHI and PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PHI and PII was stored, used, and exchanged, and those in

its employ who were responsible for making that happen.

57. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI and PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PHI and PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

58. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and members of the Class's personal information and PHI and PII.

59. The risk that unauthorized persons would attempt to gain access to the PHI and PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PHI and PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PHI and PII—whether by malware or otherwise.

60. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI and PII of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

61. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PHI and PII of Plaintiff and members of the Class which actually and proximately

caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

62. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PHI and PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PHI and PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

63. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

64. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

65. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

66. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect patient PHI and PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI and PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

67. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

68. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PHI and PII.

69. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PHI and PII.

70. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

71. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' PHI.

72. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

73. Plaintiffs and Class members are within the class of persons that the HIPAA was intended to protect.

74. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiffs and the Class members.

75. Defendant breached its duties to Plaintiffs and the Class under HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PHI.

76. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

77. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

78. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

79. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PHI and PII, Plaintiff and members of the Class would not have entrusted Defendant with their PHI and PII.

80. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PHI and PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy
On Behalf of Plaintiff and the Class

81. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

82. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class Members by disclosing and exposing Plaintiff's and Class Members' PII and PHI to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

83. The disclosure of the PII and PHI is harmful and would be offensive to a reasonable person of ordinary sensibilities.

84. Defendant should appreciate that the cyber-criminals who stole the PII and PHI would further sell and disclose the PII and PHI and that the original disclosure is devastating to

the Plaintiff and the Class Members even though it may have originally only been made to one person or a limited number of cyber-criminals.

85. The tort of public disclosure of private facts is recognized in Wisconsin. Plaintiff's and the Class Members' private PII and PHI was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and knows that Plaintiff's and Class Members' PII and PHI is not a matter of legitimate public concern. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages.[3]

COUNT IV
Declaratory and Injunctive Relief
On Behalf of Plaintiff and the Class

86. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

---

[3] In Wisconsin, invasion of privacy is governed by Wis. Stat. § 895.50, which provides in relevant part: (1) The right of privacy is recognized in this state. One whose privacy is unreasonably invaded is entitled to the following relief (b) Compensatory damages based either on plaintiff's loss or defendant's unjust enrichment; and (c) A reasonable amount for attorney fees. (2) In this section, invasion of privacy means any of the following: … (c) Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed. It is not an invasion of privacy to communicate any information available to the public as a matter of public record. In order to establish a cause of action for invasion of privacy under Wis. Stat. § 895.50(2)(c), a plaintiff must prove: (1) a public disclosure of facts regarding the plaintiff; (2) the facts disclosed are private facts; (3) the private matter made public is one which would be highly offensive to a reasonable person of ordinary sensibilities; and (4) the defendant acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter, or with actual knowledge that none existed.

87. Defendant acted or refused to act on grounds that apply generally to Plaintiff and the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class within the meaning of Wis. Stat. § 803.08(2)(b).

88. Plaintiff seeks a declaration that Defendant's acts and omissions as alleged herein violate applicable state law as well as such other and further relief as may follow from the entry of such a judgment and request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PII and PHI data between Defendant and third parties unlawful.

89. Plaintiff and the Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PII or PHI without first adequately securing or encrypting it.

90. Plaintiff and the Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PII and PHI in their possession or the possession of third parties and provide it to Plaintiff and the Class Members.

91. Plaintiff and the Class Members request that the Court enter an injunction ordering that Defendant:

a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct, test, and audit Defendant's safeguards and procedures on a periodic basis;

b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

c. conduct regular checks and tests on its safeguards and procedures;

d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

e. meaningfully educate its former and current employees about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard employee PII; and

f. identify to each Class Member in writing with reasonable specificity the PII and personal information of each such Class Member that was stolen in the Data Breach.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI and PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 8th day of August, 2022.

Dated: August 8, 2022

Respectfully submitted,

By: */s/ Samuel J. Strauss*

Samuel J. Strauss (SBN 1113942)
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff